(12) INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
10 May 2001 (10.05.2001)

PCT

(10) International Publication Number
WO 01/33353 A2

(51) International Patent Classification[7]: G06F 11/00

(21) International Application Number: PCT/DK00/00616

(22) International Filing Date:
3 November 2000 (03.11.2000)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:

PA 1999 01584	3 November 1999 (03.11.1999)	DK
60/164,332	9 November 1999 (09.11.1999)	US
PA 2000 01073	7 July 2000 (07.07.2000)	DK

(71) Applicant *(for all designated States except US)*: **VIGILANTE A/S** [DK/DK]; Vermundsgade 38, DK-2100 Copenhagen Ø (DK).

(72) Inventors; and

(75) Inventors/Applicants *(for US only)*: **MUNKEDAL, Ulf** [DK/DK]; Ryparken 39 St., DK-2100 Copenhague Ø (DK). **HEJGAARD VESTERGAARD, Aage** [DK/DK]; Godsparken 164, DK-2670 Greve (DK). **NØRGAARD, Bo** [DK/DK]; Sophienborgvænget 9, DK-3400 Hillerød (DK). **VARSTED, Steen** [DK/DK]; Elmevang 28, DK-2830 Virum (DK). **NEUPART, Lars** [DK/DK]; Sveasvej 10, 3., 2, DK-1917 Frederiksberg C (DK). **GRÜNDL, Peter** [DK/DK]; Edward Griegs Gade 17, 3. th., DK-2100 Copenhagen Ø (DK). **WILLEN, Ken** [DK/DK]; Geelsdalen 14, Dk-2830 Virum (DK).

(74) Agent: **PLOUGMANN, VINGTOFT & PARTNERS A/S**; Sankt Annæ Plads 11, DK-1250 København K (DK).

(81) Designated States *(national)*: AE, AG, AL, AM, AT, AT (utility model), AU, AZ, BA, BB, BG, BR, BY, BZ, CA, CH, CN, CR, CU, CZ, CZ (utility model), DE, DE (utility model), DK, DK (utility model), DM, DZ, EE, EE (utility model), ES, FI, FI (utility model), GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KR (utility model), KZ, LC, LK, LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW, MX, MZ, NO, NZ, PL, PT, RO, RU, SD, SE, SG, SI, SK, SK (utility model), SL, TJ, TM, TR, TT, TZ, UA, UG, US, UZ, VN, YU, ZA, ZW.

(84) Designated States *(regional)*: ARIPO patent (GH, GM, KE, LS, MW, MZ, SD, SL, SZ, TZ, UG, ZW), Eurasian patent (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European patent (AT, BE, CH, CY, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE, TR), OAPI patent (BF, BJ, CF, CG, CI, CM, GA, GN, GW, ML, MR, NE, SN, TD, TG).

Published:
— *Without international search report and to be republished upon receipt of that report.*

For two-letter codes and other abbreviations, refer to the "Guidance Notes on Codes and Abbreviations" appearing at the beginning of each regular issue of the PCT Gazette.

WO 01/33353 A2

(54) Title: TESTING OF ACCESS SECURITY OF COMPUTERS ON A DATA COMMUNICATION NETWORK

(57) Abstract: A method of operating a computer system as well as the computer system is disclosed for testing the access security of computers being connected to a data communication network. The security of the computer system itself is improved by performing individual parts of a complete test from one or more test computers temporarily connected to a scheduler computer to which the partially test results are communicated from the test computer(s). Thereby, the risk of unauthorised access to the highly sensitive test data is diminished. A series of successive tests comprises a scanning for open communication ports followed by an identification procedure for identifying the communication protocols of the communication ports, after which the access security of the open, identified communication ports is tested.

TESTING OF ACCESS SECURITY OF COMPUTERS ON A DATA COMMUNICATION NETWORK

The present invention relates to a method of operating a computer system for testing the access security of computers being connected to a data communication network, preferably a public network such as the Internet. The security of the computer system itself is improved by performing individual parts of a complete test from one or more test computers that are only temporarily connected to a scheduler computer from which the execution of the complete test is controlled and to which the partially test results are communicated from the test computer(s). The invention also relates to the computer system for performing the method as well as the computer programme product in a computer readable form being suitable to enable general purpose computers to perform the method.

In particular, the computer system can perform a series of successive tests on the external computer to be tested, the series comprising a scanning for open communication ports of the external computer followed by an identification procedure for identifying the communication protocols of the identified open communication ports, after which the access security of the open communication ports is tested by means of various test applications by utilising the obtained knowledge concerning the communication ports.

Furthermore, the present invention relates to a method of identifying the communication protocols of identified open communication ports on an external computer which is accessed vi a public data communication network. A possible response is received from the port when the connection is established and a dialog between the identifying computer system and the external computer is taking place, comprising at least one response from the external computer but usually a series of commands from the identifying computer system and a series of responses from the external computer, from which response(s) the identity of the protocol is determined.

A further aspect of the present invention relates to a systematic and automatic scanning of vulnerabilities of data communication devices with respect to reaction to receiving invalid data communication packages so as to test the robustness of the devices.

Background of the invention

A number of commercially available software applications are known by means of which the access security of a computer system may be tested via a public data communication network. These applications and the intended use of them include certain drawbacks. The procedure of testing access security is in itself endangering the security of the computer system since sensitive knowledge about the system is obtained from the test and it may be necessary to provide sensitive information about the computer system to the test application in order to achieve a useful test result.

One application for testing access security of a computer system via an external data communication connection is disclosed in the patent US 5,892,903. The system and method includes a IP spoofing generator, a port map service generator and several other parts that individually or as a group can detect vulnerabilities on a computer network. Another such application is disclosed in WO 00/38036 in which results from one scan module may be transferred as input to another module so as to improve the quality of the testing. An old and well-known application for system administrators to analyse networks and test security is SATAN. Another application that is used by system administrators for testing computer security from within the computer network is disclosed in WO 99/56195 in which a database of known vulnerabilities is updated regularly and is accessed by the modules of the application performing the testing.

The above mentioned references provides plenty of background material for the present disclosure, but the two systems for testing access security from the outside does not contain any measures or means for enhancing the security of the computer system performing the testing.

The tests have to be performed from a computer with has an unprotected connection to the public data communication network because a dialog between the external computer to be tested and the test computer on which the application is executed must be enabled. Thus, the test computer cannot at the same time have a high level of access security and the risk that sensitive knowledge about the tested system it obtained by non-authorised third parts is not negligible.

Another drawback of the known software application is that they are only known to be adapted to perform testing of a number of predefined data communication ports using the standard communication protocol of each given port, such as testing port 80 using HTTP (Hyper Text Transfer Protocol) and testing port 21 using FTP (File Transfer Protocol). However, it is not unusual that computer systems have non-standard usage of ports for a given communication protocol, often caused by various hardware and software of the individual system which infringes on the standard usage of the ports. Such systems may not be fully tested for access security by means of the known applications unless a modification is provided for.

Brief description of the invention

The present invention is advantageous over the known applications for testing the access security of computers connected to the Internet because a high security level is provided for as well as flexibility with respect to possible operating systems of test applications to be integrated into the system according to the present invention.

It is an object of the present invention to provide a method of operating a computer system for examining the access security of data communication ports of an external computer in which a high security is obtained as well as such a computer system. This is in general obtained from the present invention by performing on separate computers the examinations or tests via a public or private data communication network and the overall control of tests, the separate computers having only temporarily a data communication connection established there between.

It is another object of the present invention that the examination of access security is adapted to examine given ports for identifying their communication protocols prior to the actual examination for access security and optionally also to examine for port status, i.e. whether ports are open or closed, prior to the examination for communication protocols.

It is a yet further object of the present invention so provide method of operating a computer system for identifying the communication protocol of data communication ports of an external computer system as well as a such a computer system and a computer program product for performing such method.

It is a still yet further object of the present invention to provide a method of testing the vulnerability of devices for performing data communication

Additional objects of the present invention will be apparent from the following description.

Thus, the present invention relates to a method for operating a computer system for examining the access security of communication ports of an external computer, the method comprising the steps of

(1) retrieving, by means of a first computer of the computer system, a unique data communication address of the external computer, at least one unique communication port identification as well as the data communication protocol of each of the at least one communication port from data storage means associated with the first computer,

(2) establishing a data communication connection between the first computer and a second computer of the computer system via a data communication network,

(3) communicating the data communication address of the external computer, the communication port identification(s) as well as the data communication protocol(s) of the communication port(s) from the first computer via the data communication connection to said second computer, whereupon the data communication connection between the first computer and said second computer is closed,

(4) establishing a data communication connection from said second computer via a data communication network to the communication port of the external computer in accordance with the previously communicated data communication address of the external computer,

(5) examining the access security of the communication port(s) of the external computer by means of a software application being designed thereto and being executed by said second computer, whereupon the data communication connection between said second computer and the external computer is closed,

(6) generating a set of test result data representing the outcome of said examination and storing the set of test result data within data storage means associated with said second computer,

(7) establishing a data communication connection between the first computer and said second computer of the computer system via a data communication network,

(8) communicating the set of test result data from said second computer via the data communication connection to the first computer, whereupon the data communication connection between the first computer and said second computer is closed, and

(9) storing said test result data within data storage means associated with the first computer.

By the term "data communication port" is understood communication endpoints defining all possible communication entry points into a computer or computer system, in particularly TCP ports and TCP/UDP ports and communication ports derived or further developed from these definitions but also covering other points of communication operated according to a communication protocol.

The data storage means associated with the various computers described may are computer-readable media such as e.g. magnetic discs or tapes, optical discs, CD-ROMS, RAM circuits, etc., each media being in permanent or temporarily data-communication contact with the computer in question, the computer having a central processing unit and input and output units.

The data communication network may be a private network to which only a limited and defined group of computers may have access or preferably a public data communication network. The public data communication network is understood as a network to which an undefined group of users may obtain access or are in permanent connection with via computers, the network may further include one or more local networks and/or one or more wide area network.

The computer system may in order to be more flexible with respect to the inclusion of applications available from third parties comprises at least two second computers being operated by means of different common standard computer operating systems. In a preferred embodiment, the computer system comprises for a number of operating systems at least two second computers or test computers operated by means of the same common standard computer operating systems, such as Linux, Windows NT, Unix variants etc.

It is also preferred that the computer system comprises at least two second computers which may operate concurrently according to the present method so that different or identical test applications may be executed simultaneously or concurrently. The at least two second computers may operate concurrently employing an identical data communication address of the external computer, identical communication port

identification(s) as well as identical data communication protocol(s) of the communication port(s) so that the port(s) are examined by more than one test application concurrently or by the same application from two computers concurrently.

Since the actual definition of data communication protocols of the various ports of a given external computer may deviate from the standard settings, it is an advantage that the present method comprises a port identification procedure being performed by a second computer of the computer system prior to the step (1) of retrieving data from said data storage means associated with the first computer of the computer system, the port identification procedure identifying data communication protocol(s) of communication port(s) of the external computer and produce an output accordingly.

The port setting, meaning which ports are open for data communication, may be predefined in the computer system or may be given from an external source. However, since the actual port setting of a given external computer also may deviate from the standard definition, it is a further advantage that the present method comprises a port examining procedure being performed by a second computer of the computer system prior to the port identification procedure, the port examining procedure being adapted to detect whether data communication via each of the plurality of communication ports of the external computer is enabled and produce an output accordingly, said output being significant for which ports of the external computer the data communication protocols are identified by means of the port identification procedure.

It is of great value for the quality of the result of many test cases and an advantage that knowledge about the file structure and the location of particular files or types of files on the external computer is known prior to the execution of the test case. These information may be obtained by accessing the external computer through a communication port dedicated to communication using a suitable protocol, such as HTTP. The communication port may be selected because it is a de facto standard that the port is dedicated to the protocol that is preferred or it may have been detected during the above mentioned port examining procedure. Thus, the method may comprise a data location procedure being performed by a second computer of the computer system prior to the step (1) of retrieving data from said data storage means associated with the first computer of the computer system, the data location procedure identifying the location of specific types of data files on data storage means associated with the external computer and produce an output of

test result data accordingly to the first computer of the computer system to be used for subsequent examinations of access security of the external computer to which the test result data pertains.

In particular the data location procedure may comprise the steps of

retrieving, by means of a first computer of the computer system, a unique data communication address of the external computer from data storage means associated with the first computer,

establishing a data communication connection between the first computer and the second computer of the computer system via a data communication network,

communicating the data communication address of the external computer from the first computer via the data communication connection to said second computer, whereupon the data communication connection between the first computer and said second computer is closed,

establishing a data communication connection from said second computer via a data communication network to the external computer in accordance with the previously communicated data communication address of the external computer,

examining data storage means associated with the external computer so as to identify the location of specific types of data files on data storage means associated with the external computer by means of a software application being designed thereto and being executed by said second computer, whereupon the data communication connection between said second computer and the external computer is closed,

generating a set of test result data representing the outcome of said examination and storing the set of test result data within data storage means associated with said second computer,

establishing a data communication connection between the first computer and said second computer of the computer system via a data communication network,

communicating the set of test result data from said second computer via the data communication connection to the first computer, whereupon the data communication connection between the first computer and said second computer is closed, and

storing said test result data within data storage means associated with the first computer to be used for subsequent examinations of access security of the external computer to which the test result data pertains.

In order to be able to examine the access security of a port dedicated to encrypted communication, the computer system may be provided with an encryption key, that be a public key, a default key or a specific key for the communication Thus, if the data communication protocol of the communication port of the external computer involves encryption, an encryption key is communicated in step (3) from the first computer to the second computer, and said encryption key is used at least for encrypting communication from the second computer to the external computer during the examination in step (5).

It is an advantage from a security point of view that the test results only may be retrieved from the first computer from an external computer via a secure data communication connection, such as a connection in which the exchanged data are encrypted. A preferred embodiment of the present invention includes the initial steps of

retrieving from data storage means associated with a third computer of the computer system at least one unique data communication address of an external computer,

establishing a data communication connection between the third computer and said first computer via a data communication network,

communicating said at least one data communication address of the external computer(s) from the third computer via the data communication connection to the first computer, whereupon the data communication connection is closed, and

storing said at least one data communication address within data storage means associated with the first computer,

after which initial steps the remaining of the method is performed for said communicated at least one data communication address, the method further comprising the final steps of

establishing a data communication connection between the third computer of the computer system and said first computer via a data communication network,

retrieving test result data relating to at least one of said communicated at least one data communication address from data storage means associated with the first computer,

communicating said retrieved test result data from the first computer via the data communication connection to the third computer, whereupon the data communication connection is closed,

storing said test result data within data storage means associated with the third computer,

establishing a data communication connection between an external computer and the third computer via a data communication network,

retrieving said test result data from data storage means associated with the third computer,

encrypting said retrieved test result data by means of a first encryption key, and

communicating said encrypted test result data from the third computer via the data communication connection to the external computer, whereupon the data communication connection is closed.

The set of test result data may further more be deleted from the data storage means associated with said first computer immediately upon the set of data has been communicated to the third computer so as to further enhance the security level of the computer system. Likewise, the set of test result data may be deleted from the data storage means associated with said third computer immediately upon the set of data has been communicated to the external computer.

The unique identification of at least one communication port of the external computer may be provided to the first computer by retrieving said identification from data storage means associated with the third computer during the initial retrieving step, said unique identification of at least one communication port being communicated to the first computer during the initial communication step. Likewise, the data communication protocol(s) of at least one communication port of the external computer may be retrieved from data storage means associated with the third computer during the initial retrieving step, said data communication protocol(s) being communicated to the first computer during the initial communication step. These identifications and protocols may have been predefined or may have been obtained from a third, external source and the tests may be performed using these identifications and protocols solely or in combination with identifications and protocols obtained by the computer system by examination of the external computer as described above.

Test specification data relating to the type of examination to be performed of the access security of the communication port(s) of the external computer may also be retrieved from data storage means associated with the third computer during the initial retrieving step, said test specification data being communicated to the first computer during the initial communication step. These test specification data may have been predefined or may have been obtained from a third, external source.

It is advantageous that the customer knows when the scanning of the customers external computer is performed because of the load on the computer during the examinations and because the computer needs to be fully operational. The initial steps of the method may accordingly further comprise the step of

retrieving from data storage means associated with the third computer of the computer system a predetermined start time and a predetermined end time,

the method further comprising the step of

controlling the examination of the access security of step (5) so that the examination is performed between said predetermined start time and said predetermined end time.

Alternatively to the usage of a third computer to provide a secure route for communicating the test result data to an external computer, the method may comprise the steps of

establishing a data communication connection between an external computer and the first computer via a data communication network,

retrieving said test result data from data storage means associated with the first computer,

encrypting said retrieved test result data by means of a first encryption key, and

communicating said encrypted test result data from the first computer via the data communication connection to the external computer, whereupon the data communication connection is closed.

The set of test result data may additionally be deleted from the data storage means associated with said first computer immediately upon the set of data has been communicated to the external computer.

The above-mentioned port identification procedure may in a preferred, particular embodiment of the present invention comprise the steps of

(a) retrieving from data storage means associated with the first computer a unique data communication address of an external computer,

(b) establishing a data communication connection between the first computer and a second computer of the computer system via a data communication network,

(c) communicating the data communication address of the external computer from the first computer via the data communication connection to said second computer,

whereupon the data communication connection between the first computer and said second computer is closed,

(d) establishing a data communication connection from the second computer via a data communication network to a communication port of the external computer,

(e) receiving a possible first response via the data communication connection from the external computer,

(f) evaluating the first response, which may be empty, by use of a first set of information stored within data storage means associated with the second computer and relating to first responses from communication ports, said evaluation producing a first evaluation result of one of the following types:

i) the protocol cannot be identified by the present identification procedure,

ii) the identity of the protocol is identified, and

iii) further communication is required for protocol identification,

(g) performing, in case the first evaluation result is of type iii), a process comprising the following steps:

(h1) retrieving, in case the first evaluation result is of type iii), a second command from data storage means associated with the second computer,

(h2) communicating said second command from the second computer via the data communication connection to the communication port,

(h3) receiving a second response via the data communication connection from the external computer,

(h4) evaluating the received second response by use of a second set of information stored within data storage means associated with the second computer and relating to second responses from communication ports, said evaluation producing a second evaluation result,

(j) generating a set of port identification data representing the outcome of said identification procedure and storing the set of port identification data within data storage means associated with said second computer,

(k) establishing a data communication connection between the first computer and said second computer of the computer system via a data communication network, and

(l) communicating the set of port identification data from said second computer to the first computer, whereupon the data communication connection between the first computer and said second computer is closed.

The first response to the establishment of a data communication connection to a port may be empty, that is no response, which e.g. is the case for ports using HTTP, whereas ports using e.g. FTP provide a response upon the establishment of a connection. It should be noted that the responses from different ports using the same data communication protocol to a given command are not necessarily identical. The responses may comprise additional information about the manufacturer of the hardware of software, about the given computer or parts of the standard responses may have been removed or suppressed.

The set of port identification data may for security reasons be deleted from the data storage means associated with said second computer immediately upon the set of data has been communicated to the first computer.

The second evaluation result is, according to a further preferred embodiment of the present invention, of one of said types of first evaluation results, and the method further comprises the step of performing, in case the second evaluation result is of type iii), a process comprising steps being similar to (h1) to (h4) involving a third command, a third response, a third set of information and a third evaluation result. The method may further comprise one or more further processes comprising steps being similar to (h1) to (h4) depending on how many responses are necessary to determine the identity of the protocol.

The protocols are in general common standard data communication protocols but may also be special protocols utilised by a very limited number of communication applications.

The identification process may be performed for the individual port in a tree-structured manner, according to which the same process may lead to any of the protocols known by the system depending on the responses from the port so that the commands to be communicated to the port are selected based on the previously received responses. However, in order to perform a time-efficient identification process of the protocol, it is advantageous that a plurality of said identification processes are performed concurrently employing an identical unique data communication address of the external computer as well as an identical unique communication port identification, each of the plurality of identification processes employing command(s) and set(s) of information being specific for a given data communication protocol so as to test the communication port of the external computer for a plurality of different data communication protocols concurrently.

When a positive identification is obtained, i.e. when an evaluation result of type ii) is achieved from any of the plurality of identification processes, ongoing identification processes of the plurality of identification processes are in a preferred embodiment terminated.

The identification process may be repeated automatically with a new port identification from a series of stored port identification of the same external computer, in which case the method further comprises the step of

(m) retrieving from data storage means associated with the second computer a new unique communication port identification,

after which the steps according to the method with the exception of steps (a)-(c) are repeated using the new unique communication port identification instead of the prior port identification.

The identifications of the ports of which the data communication protocol is to be identified by means of the described process may be obtained from a port scanning process being integrated in the protocol identification process or being performed simultaneously with the protocol identification process on the same second computer. However, it is an advantage that the two processes are separated in order to enhance the security level of the computer system. The port identification may alternatively be obtained from a source being external to the computer system and being provided to the first computer by other means. Thus, according to a preferred embodiment of the present invention, unique identification of at least one communication port of the external computer is retrieved from data storage means associated with the first computer during step (a), said unique identification of at least one communication port being communicated to the second computer during step (c), said unique identification of at least one communication port being significant for which ports of the external computer the data communication protocols are identified by means of the port identification procedure.

While performing the procedure for identification of communication ports or the procedure for examination of the communications ports there is a risk that a system for preventing unauthorised access to the tested computer system, known as Intrusion Detection and Protection System, detects that an attack from the test computer is in progress and shuts out the test computer from communicating with the tested computer system, so-called

"shunning". The attack may be recognised from the order of the ports to which contact is made from a particular IP address, a successive order of ports, such as 1, 2, 3, 4, 5 ... or from the attempted contact to unusual ports that commonly are not used for communication. This shunning might result in false test results and it is therefore useful to examine the plurality of communication ports in a non-successive order designed to prevent a safety system of the external computer from recognising a systematic examination.

It is also useful to arrange communication ports having a communication protocol assigned therewith according to a common or de facto communication standard at the beginning of the non-successive order. Furthermore, the types of ports may be mixed in order to prevent shunning, so that communication ports not having communication protocol assigned therewith according to the common or de facto communication standard are arranged in the non-successive order with less than four, preferably less than three and most preferred less than two such communication ports between the communication port in question and a communication port having a communication protocol assigned therewith according to the common or de facto communication standard.

Finally, it may also be advantageous that communication ports not having communication protocol assigned therewith according to the common or de facto communication standard are arranged at the end of the non-successive order. Thereby, a possible shunning of the IP address will most likely not be effectuated until most of the communication ports have been examined.

It is also in order to evaluate the results of the examination of the communication ports advantageous to include the following check for shunning prior to the first performance of step (d) in a method wherein step (m) and the thereof following port identification procedure are performed for a multitude of communication port of the external computer. The check may additionally or alternatively be performed prior to the examination of the plurality of communication ports. The check method comprises the steps of

(c1) establishing a data communication connection from the second computer via a data communication network to one or more predetermined communication port(s) of the external computer,

(c2) receiving a possible first response from each of the predetermined communication port (s) via the data communication connection from the external computer, and

(c3) storing the first response(s) from the predetermined communication port(s) within data storage means associated with said second computer,

the method further comprising the step of at least once during or after the performance of the multitude of identification procedures of communication ports,

retrieving the stored first response(s) from the data storage means associated with the second computer,

repeating steps (c1) and (c2), and

performing a comparison of the obtained first response(s) from the predetermined communication port(s) with the retrieved first response(s) so as to detect a disruption of the ability to establish data communication connections between the second computer and the external computer.

It is preferred that in order to detect a disrupted data communication connection, the procedure of detecting a possible disruption is performed after the examination of each communication port, so as to avoid false test results.

In order to have a full examination procedure executed even if shunning may be effectuated against the examining second computer the following steps may be included into the present method:

the procedure of detecting a possible disruption is performed after the examination of each communication port,

the port examining procedure is halted upon a detection of disruption of the ability to establish data communication connections between the second computer and the external computer,

where after the examination is resumed on another second computer of the computer system excluding the communication port being examined immediately prior to the disruption was detected.

The non-successive order of the communication ports may furthermore be arranged according to known shunning-ports, that is communication ports that from experience are known to cause a shunning and/or according to known shunning-sequences, that is known sequences of scanning of communication ports known to cause shunning. This empirical knowledge may be collected and used in an automatic and organised manner by means of the computer system disclosed. Thus, the present method may comprise the steps of

store information about the order of examination of communication ports immediately prior to disruptions within data storage means of the computer system for a plurality of examinations of communication ports of external computers,

performing an analysis of said information by means of the computer system so as to identify a set of individual communication ports and sequences of communication ports being likely to cause a disruption and a data set in accordance herewith is stored within data storage means of the computer system, and

arranging the non-successive order for subsequent examination of communication ports so that said individual communication ports are arranged at the end of the non-successive order and said identified sequences of communication ports are avoided.

The above-discussed port examining procedure may in a particular embodiment of the present invention comprise the steps of

retrieving, by means of the first computer, a unique data communication address of the external computer from data storage means associated with the first computer,

establishing a data communication connection between the first computer and a second computer of the computer system via a data communication network,

communicating the data communication address of the external computer from the first computer via the data communication connection to said second computer, whereupon the data communication connection between the first computer and said second computer is closed,

establishing a data communication connection from said second computer via a public data communication network to the external computer in accordance with the previously communicated data communication address of the external computer,

examining a plurality of communication ports of the external computer to detect whether data communication via each of the plurality of communication ports is enabled, said examination being performed by means of a software application being designed thereto and being executed by said second computer, whereupon the data communication connection between said second computer and the external computer is closed,

generating a set of port status data representing the outcome of said examination and storing the set of test result data within data storage means associated with said second computer,

establishing a data communication connection between the first computer and said second computer of the computer system via a data communication network, and

communicating the set of port status data from said second computer to the first computer, whereupon the data communication connection between the first computer and said second computer is closed,

the communicated set of port status data being significant for which ports of the external computer the data communication protocols are identified by means of the port identification procedure.

The set of port status data may for security reasons be deleted from the data storage means associated with said second computer immediately upon the set of data has been communicated to the first computer.

Likewise, the set of test result data may be deleted from the data storage means associated with said second computer immediately upon the set of data has been communicated to the first computer.

The present method may be performed on a private data communication network of data communication connections but the method is mainly directed towards the situations where the data communication connection(s) between the second computer and a communication port of the external computer is established via a public data communication network because the risks of unauthorised intrusion is generally higher when a public network is involved.

To verify that the computer being examined actually is accessible from the computer system during the examination it is useful to test the communication pathway. This may be done e.g. by sending a request from the computer system to a port of one of the computers on the level of the examined computer from which port, e.g. a HTML port, a reply is issued if the communication pathway is operational. Alternatively, if the external computer system does not have such ports, the external computer system may send a request through the communication pathway to the testing computer system or a computer associated therewith. Thus, the method may if the external computer is as part of an external computer system having a common data communication pathway, typically comprising a Router and a Firewall, through which all data communication to and from computers of the external computer system passes, further comprise steps of

establishing a data communication connection between a computer of the computer system and a computer of the external computer system, and

at least once prior to or during the performance of an examination of the access security of the communication port(s) receiving data from said computer of the external computer system so as to verify that the common data communication pathway of the external computer system is functioning.

In order to obtain material to form a statistical basis for a performance evaluation of a new test case that have been included into the computer system performing the present method, it may be included that the generated set of test results is stored within data storage means associated with the computer system for subsequent evaluation of the employed software application for examining the access security if said software application has been employed less than a predetermined number of times by the computer system, whereupon a counter within the computer system and pertaining to said software application is advanced with one step.

According to another aspect of the present invention a method is disclosed for operating a computer system for regularly repeated examination of the access security of communication ports of a plurality of external computers, wherein the computer system comprises a database stored on data storage means of the computer system, the database comprising record files of characteristics of each of the plurality of external computer systems as well as schedule data relating to a desired scheduling of said regular repeated examination, the method comprising the step of examining the access security of communication ports of each of the external computers on a regular basis according to the schedule data by means of the method according disclosed above.

In a particular embodiment of this method, it includes that a new partial scanning is performed for registered customers when a new vulnerability is discovered. Thus, the method further comprising the steps of

receiving input data relating to a specific vulnerability of the access security of communication ports of computers as well as test specification data for the type of examination to be performed of the access security of the communication port(s) of the external computer to test for the specific vulnerability, and

examining the access security with respect to the specific vulnerability according to the present method for each of the plurality of external computers without interfering with the scheduled regularly repeated examination of the access security.

Furthermore, a matching may be performed between the system data of the customers and the known data of the vulnerability and a separate scanning for the particular vulnerability is performed. Thus, the method further comprises the steps of

receiving input data relating to a specific vulnerability of the access security of communication ports of computers having a given set of characteristics as well as test specification data for the type of examination to be performed of the access security of the communication port(s) of the external computer to test for the specific vulnerability,

searching the database so as to select a subset of the plurality of external computers based on a matching of the characteristics stored in the database and the set of characteristics given in the receiving input data, and

examining the access security with respect to the specific vulnerability according to the present method for each of the external computers of the selected subset without interfering with the scheduled regularly repeated examination of the access security.

Also, the customer or another person or entity acting on behalf of the customer may have the opportunity to accept or refuse the performance of the additional scanning. Thus, the step of examining the access security with respect to the specific vulnerability may be preceded by the steps of

producing a request from the computer system to an external entity via a public data communication network, the request relating to the performance of said examination of one or more of said plurality of external computers, and

receiving a positive reply from the external entity to the request.

The request and the following reply may according to the present invention e.g. be sent and received via a computer communication connection, a telephone connection using wires and/or wireless transfer means and employing voice response, all constituting a public data communication network as stated above.

Some of the test result, in particular the results from port identification procedures, port examining procedures and data location procedures, may be stored within the computer system for being reused at subsequent examination, in particular examination for a single new test case. Thus, the present method may comprise that at least a part of the set of test result data generated by the regularly repeated examination of the access security of each of the plurality of external computers is stored on data storage means of the

computer system for being retrieved and used for subsequent examinations of access security of the external computer to which the test result data pertains.

A specific test case or software application for testing the access security may be a test case investigating the likeliness of the external computer to become blocked by an attack, to give a so-called "Denial of Service". The attacks may typically be to repeatedly request the opening of a communication connection without finishing the handshake between the two computers according to the communication standard or send a huge amount of communication packages to the external computer, so-called "flooding" or send invalid data packets. Thus, the execution of the software application employed in step (5) may comprise the steps of

(5.1) repeatedly performing a specified communication with one of the communication port of the external computer, and

(5.2) determine whether the communication port in question provides a response to the communication.

This particular test case is very important to include as it is a common step in many strategies of acquiring illegal access to an external computer to provoke a Denial of Service from one or more ports of the external computer.

To make sure that the Denial of Service is caused by the present test case, the method may include a control by repeating the test, so that the method further comprises the step of

(5.3) repeating step (5.1) after a predetermined time period in case it is determined in step (5.2) that the communication port in question does not respond.

It may be an advantage if the computer system is able to be contacted by the customer or a person or entity representing the customer and halt or alternatively repeat the test. Thus, the computer system performing the method may be adapted for having a communication connection established to an external entity via a public data communication network and receiving and executing instructions for ending the execution of step (5.1) or for repeating step (5.1). The communication network may be the ordinary data communication network of the external computer. Alternative or additionally, the communication connection may be established via a telephone line using data

communication or voice response, in case the ordinary communication connection from the external computer is blocked because of the provoked Denial of Service.

Likewise, the computer system may be adapted for establishing a second data communication connection via a data communication network under the conditions that

it is determined in step (5.2) that the communication port in question does not respond, and

the communication port in question does not respond a predetermined time period thereafter,

and producing a communication accordingly so that the customer or a person or entity representing the customer is made aware of the fact that the external computer is blocked for communication.

The present invention also relates to a computer system comprising at least two general purpose computers having one or more computer programs stored within data storage means associated therewith, the computer system being arranged for as well as being adapted for performing the method or methods according to the present invention and described above including each of the described possible combination of steps and procedures.

The system is generally described as having a single computer performing as the third computer of the method, but it is within the scope of the present invention that the computer system comprises at least two computers each being arranged for as well as being adapted for performing as a third computer according to the method, said at least two computers having a common data storage means associated with each of said at least two computers, each of said at least two computers being adapted for storage of test result data within said common data storage means as well as being adapted for retrieval of test result data from said common data storage means.

The computer system may likewise comprise at least two computers each being arranged for as well as being adapted for performing as a first computer according to the method.

The present invention further relates to a method for operating a computer system for identifying data communication protocol(s) of communication port(s) of an external computer, comprising an identification procedure having the steps of

(a) retrieving from data storage means associated with the computer system a unique data communication address of the external computer as well as a unique communication port identification,

(b) establishing a data communication connection from the computer system via a data communication network to a communication port of the external computer in accordance with the information retrieved in step (a),

(c) receiving a first response via the data communication connection from the external computer,

(d) evaluating the received first response, which may be empty, by use of a first set of information stored within data storage means associated with the computer system and relating to first responses from communication ports, said evaluation producing a first evaluation result of one of the following types:

i) the protocol cannot be identified by the present identification procedure,

ii) the identity of the protocol is identified, and

iii) further communication is required for protocol identification,

(e) performing, in case the first evaluation result is of type iii), a process comprising the following steps:

(f1) retrieving, in case the first evaluation result is of type iii), a second command from data storage means associated with the computer system,

(f2) communicating said second command from the computer system via the data communication connection to the communication port,

(f3) receiving a second response via the data communication connection from the external computer, and

(f4) evaluating the received second response by use of a second set of information stored within data storage means associated with the computer system and relating to second responses from communication ports, said evaluation producing a second evaluation result. This aspect of the present invention is described in the above as a part of the method for examining access security but may also be regarded as an invention in itself. The second evaluation result may, as previously described, be of one of said types of first evaluation results, and the method further comprises the step of performing, in case the second evaluation result is of type iii), a process comprising steps being similar to (f1) to (f4) involving a third command, a third response, a third set of information and a third evaluation result. The method may optionally comprise one or more further processes comprising steps being similar to (f1) to (f4) and at least some of the protocols are preferably common standard data communication protocols and the method may

furthermore according to be invention comprise the characteristics as given in the above description in connection with the method for examining access security.

The present invention also relates to a computer system comprising at least one general purpose computer having one or more computer programs stored within data storage means associated therewith, the computer system being arranged for as well as being adapted for performing the method of identifying data communication protocol(s) of communication port(s) of an external computer as disclosed above. The present invention furthermore relates to a computer program product being adapted to enable a computer system comprising at least one general purpose computer having data storage means associated therewith and being arranged suitably to perform said method.

It has been found by the inventors that some electronic equipment comprising a device for data communication via a data communication network, such as routers, printers, computers, telefaxes etc. may have that device deactivated or even destroyed by having an invalid data packet sent to the device via the data communication network. This may happen accidentally or on purpose to harass the owner or users of the equipment. Thus, it is important to test new and existing devices for vulnerability to such data packages and t it is furthermore important to test it in an automated and a systematic manner.

Thus, the present invention relates in a further aspect to a method for testing the vulnerability of a device for performing data communication via a data communication network by using a given common data communication standard, comprising the successive steps of

(a) establishing a data communication connection between a computer and the device via a data communication network,

(b) generating a data package in which the combination of attributes is invalid according to the given common data communication standard,

(c) communicating said data package from the computer to the device,

(d) detecting whether the device is able to issue a proper response to a valid data communication from the computer system, and

(e) repeating step (b) with a new invalid combination if the device was tested positive in step (d).

The step (b) is preferably repeated for a plurality of invalid combinations so that the substantially all possible invalid combinations are tested.

Such invalid combinations may be that the defined option length of an ICMP packet is shorter than the actual option length, such as a defined length of 0 (zero). Another invalid combination is to state the same MAC address as the target and the sender in an etherpacket. The possible invalid combinations depend on the communication standard of the devices.

Detailed description of an embodiment according to the invention

The protection of sensitive information is necessarily a key issue when designing a computer system for testing the security of computers connected to a public data communication network. Other important design parameters are robustness of the system and flexibility meaning that test applications from various vendors can be integrated into the system. The design of the embodiment of a computer system according to the invention is described in details below and by the accompanying Figs. 1-3, of which

Fig. 1 shows the overall design of the computer system,

Fig. 2 shows the details of the testing part of the system comprising a computer being the scheduler and a number of test computers performing the actual tests, and

Fig. 3 is a flow diagram of the port identification procedure.

The computer system comprises a system controller which is the computer controlling the overall operation of the computer system and handling the communication with customers via a secure data communication connection to the Internet. The secure data communication connection, such as a secure web server protocol (HTTPS) using a secure socket layer (SSL), enables encrypted communication with the customers through which orders for tests are received by the computer system and the test results are distributed. A high security level is furthermore obtained by a so-called "firewall" between the data communication connection to the Internet and the system controller. This is preferably the only permanent data communication connection between the computer system and the Internet, optionally together with an ordinary HTTP connection to a restricted part of the computer system for public informational purposes.

The system controller can establish a data communication connection to the scheduler, in the present embodiment also known as Robert, either via a private data communication network or via a public data communication network, such as the Internet, in which latter case a secure data communication connection is used. This data communication connection is only established temporarily for the transfer of order files from the system controller to the scheduler and for retrieving test result files from the scheduler and the data communication may only be established by request from the system controller in

order to prevent unauthorised access to the system controller via the scheduler. The order file comprises one or more unique data communication addresses, IP-addresses, of external computer systems to be tested as well as identification of the tests (or tasks) to be performed on the external computer systems and optionally an internal order identification. The result file comprises the results of the tests that have been performed as well as an identification of the external computer systems that have been tested, either in the form of the IP-addresses of the external computer systems or in the form of the optional internal order identification. The security of the system is increased by the use of an internal order identification because it will make it more difficult for an unauthorised external intruder to link the test results to the tested computer systems.

The scheduler can establish data communication connection with a number of test computers from which the actual tests of the external computer systems are performed. As with the connection between the system controller and the scheduler, this data communication connection may be established either via a private data communication network or via a public data communication network, such as the Internet, in which latter case a secure data communication connection is used. This data communication connection is only established temporarily for the transfer of test order files from the scheduler to the test computer and for retrieving test result files from the test computers and the data communication may only be established by request from the scheduler in order to prevent unauthorised access to the system controller via the test computers. The scheduler determines the order of which the various tests are performed and directs test results from some tests into order files of a succeeding test, such as directing the result of a test that scan an external computer for open ports to be input data in a test order file for a test for determining the data communication protocol of open ports, of which test or task the output in a test result file is directed to a test order file for a number of commercially available test applications for testing the access security of ports of known communication protocols. The scheduler is also able to include test in a job started by an order file from the system controller, which tests are not stated explicitly in the order file but only implicitly, such as a open port scanning is understood to be performed prior to an explicitly stated test for determining the data communication protocol of open ports.

The test computers (or test engines) run a number of different operating systems, such as Linux, Windows NT, Unix, etc., in order to enable the computer system to execute commercially available test applications that are designed to be executed under the

different operating system and thus making the computer system more flexible. Each test application is installed on at least two different test computers in order to make the system more robust for individual break-downs of test computers, so that an order from the system controller may be executed if one (or more) of the test computers is unable to perform a given test. The test computers are able to establish data communication connections with external computers (or host computers) via a public data communication network, such as the Internet via which connections the tests are performed.

A vendor of the present system allows a customer to access the system controller via a secure data communication connection and provides the customer with a user identification and a password for entering the system controller. When a job, consisting of a number of tests to be performed on one or more external computer systems defined by their IP addresses, is ordered by the customer from the computer system, a notification is issued from the system controller to the vendor via the public communication network and the job is not effectuated before the elapse of a predefined time period, such as 24 hours, in order to give the vendor a reasonable response time to cancel the job if it turns out to be ordered by a non-authorised third part, is requested to be effectuated on an external computer not belonging to the customer or comprises another irregularity. Alternatively, the job is not effectuated until the vendor provides the system controller with a positive response to the ordered job. The order file is then created by the system controller, a data communication connection is established with the scheduler and the order file is communicated to the scheduler after which the connection preferably is closed. The scheduler has the test computers performing the required tests and a test report is created within a data storage means of the scheduler. An indication in the result file is created by the scheduler when the ordered job is completed and the system controller establish a temporary connection with regular intervals to control whether this indication has been created. In case the indication is found, the result file is transferred to the system controller and deleted from the data storage means of the scheduler to prevent a possible non-authorised intruder in the scheduler to obtain access to this highly sensitive information. A notification is issued from the system controller to the customer via the public data communication network and the customer is able to access the system controller via a secure connection and retrieve the result file comprising the outcome of the tests that have been performed.

The available tests (or tasks) comprise the following tests but more may according to the invention be added to this list:

Ping, trace route and name server lookup results.

IP TCP Port scanning for open ports, full or the first 2048 ports.

IP UDP Port scanning for open ports, full or the first 2048 ports.

SNMP scanning

Relaying of foreign e-mails.

NetBIOS tests

OS detection.

Satan and saint tests

Banner tests

Proxy tests

WebCheck test

FTP tests

Denial of service tests

nmap: A free portscanner available from http://www.insecure.org. This is used both to scan for a number of common TCP ports and to attempt to detect the operating system of the scanned host through IP fingerprinting. It runs under Linux.

traceroute: The standard Linux traceroute - freely available. It is used to determine whether the route to the scanned host can be determined using ICMP or UDP packets and to return the route if found.

icmp: A free tool that can send and receive various ICMP packets. Used to check if the scanned host answers to ping (ICMP echo request), ICMP timestamp request and ICMP netmask request.

nmscan: A port scanner developed for the present embodiment. It is used to scan for any open TCP port, and to determine the exact responses to a port scan of TCP ports 0-2048 and UDP ports 0-2048. All responses including ICMP responses to TCP packets and their source are detected.

protocolid: A protocol identifier developed for the present embodiment. It is used to determine the protocol for each of the open ports found by nmscan.

Internet Scanner NT: A commercial security scanner from ISS (http://www.iss.net). It is used to scan for a lot of known vulnerabilities.

Internet Scanner Linux: A commercial security scanner from ISS (http://www.iss.net). It is used to scan for a lot of known vulnerabilities.

CyberCop for Linux and NT: A commercial security scanner from Network Associates (http://www.nai.com). It is used to scan for a lot of known vulnerabilities.

The function of protocolid which may be regarded as an invention in itself is illustrated in Fig. 3. Protocolid is a tool designed to detect the protocol of an open TCP port. Normally a standard port is used in connection with a protocol. Thus a web server normally offers its services (using the http protocol) on TCP port 80. It is frequently seen though that a non-standard port is used - e.g. a lot of management interfaces uses the http protocol but on another port. Currently available security scanners either give no possibility of testing a non-standard port or require the port to be manually entered.

Protocolid automatically detects the protocol of an open port by trying to connect to it a number of times (one for each protocol that it is able to recognise), sending it a specific command or a number of specific commands and determining if the answers are in correspondence with the protocol.

When determining the protocol of a port, protocolid starts a new process for each protocol that it is able to recognise. Each of these new processes opens a connection to the port and sends one or more protocol-specific commands and determines from the response(s) whether the port understands the protocol in question. If the protocol is recognised the process returns 1 otherwise it returns 0. The main process of protocolid waits for the responses from the other processes and if it gets a response of 1 from any of them it kills the rest of the processes and prints the name of the process. If it gets a 0 response from all processes it prints 'unknown'. If a timeout has expired without any of the above conditions to be fulfilled it kills the processes that are not done and prints 'unknown'. The protocols currently recognised are:

http: Standard web (standard port 80)
https: Secure web (standard port 443)
ftp: File Transfer (standard port 21)
nntp: News (standard port 119)
smtp: Mail - sending (standard port 25)
pop3: Mail - mailboxes (standard port 110)
dns: Name service (standard port 53)
ldap: Directory service - address book (standard port 389)

finger: (standard port 79)
telnet: (standard port 23)
ident: (standard port 113)
imap4: Mail - mailboxes
netbios_ssn: Windows specific (standard port 139)

Protocolid is used in the computer system according to the present invention to determine the protocol that runs behind the open TCP ports to make other tools able to utilise the information. Thus Internet Security Scanner for Windows NT is able to test a web-server on a non-standard port if the port is specified in its policy. The wrapper (the interface code between Robert and a test application) that runs the scanner can then extract the result of protocolid and use it to patch the policy of the scanner before it is run.

The order file from the system controller to the scheduler is for a given embodiment of the invention a command file comprising some of or all of the following commands:

new job: Creates the job. Creating the job consists of creating the corresponding directory in \\ROBERT\OUTPUT and the jobinfo.csv file in it.

add file *<file>*:
Copies the file *<file>* from the input directory to the jobs root directory in \\ROBERT\OUTPUT. If the file is a zip file it is unzipped. To add a zip file it has to be zipped again. All files in the jobs root directory will be present in the directory where a wrapper starts executing.

add host *<host>:*
Adds the host with IP address *<host>* to the job.

add target *<target>:*
Adds the target with IP address *<target>* to the job.

add net *<net>:*
Adds the net *<net>* in the form x.x.x.x/bb to the job.

add domain *<domain>:*
Adds the domain *<domain>* to the job.

do task *<tasklist>* [*<ip>*] [*<ports>*] [*<email>*] [*<priority>*]:
Adds an order to job that will perform the tasks necessary to complete all tasks in *<tasklist>*. *<tasklist>* is either the name of a single task or a list of task names separated by commas and enclosed in square brackets []. All other arguments are optional and can be specified in

any order. <*ip*> is the IP address of a host to test, if it is not specified all hosts in the job will be tested. <*ports*> is a port or a port range to test, if it is not specified all ports are tested. <*email*> is an email address to notify when the order is complete. <*priority*> is an integer priority enclosed in parentheses ().

get status [<*uid*>]:

Returns the status of the order with uid <*uid*>. If <*uid*> is not specified the status of the job is returned.

delete job:

Moves the jobs directory in \\ROBERT\OUTPUT to a backup location.

undelete job:

Restores the jobs directory from the backup location. To actually remove the jobs directory from Robert it is necessary to perform the three commands

delete job
new job
delete job

These can all be given in the same command file.

jobcontrol <*type*> <*args*>:

Controls the way scheduling is performed for the job. <*type*> is one of:

maxrun: Set the maximum number of running tasks in the job to the number given in <*args*>.

time: Sets three time values that control when the scheduler will schedule tasks in the job.

stopmode: If <*args*> is *strict* all running tasks in the job will be stopped (killed) when scheduling in the job stops.

The jobinfo.csv file in the scheduler (Robert) is used to communicate the results of Robert between the scheduler and the test computers and between the scheduler and the system controller. The jobinfo.csv file consists of lines with a number of fields separated by tabs. The fields are

uid: An automatically generated integer. Related lines are group by uid.

wtime: The time the line was generated in the format }YYYY-MM-DD hh:mm:ss".

id:	Identifies the information in the line. Max 20 characters. E.g. *Task* for task information.
name:	A subclassification of the information in the line. Max 20 characters. E.g. *tcpscan* - the name of the task.
ipaddr:	An IP address.
ports:	A port or a port range.
value:	A value. Max 30 characters.
value2:	Another value. Max 30 characters.
addinfo:	Additional information.

Apart from addinfo the fields cannot contain tabs and control characters. In the addinfo field lines are separated by \n (a backslash followed by the letter n) and a backslash as \\ (two backslashes), as a carriage-return is not to be considered part of a line separation.

As the jobinfo.csv file is used to hold both scheduling information, job status and test results it will be changed by a lot of different tools. The following is a detailed description of the possible lines of jobinfo.csv.

When the job is created two lines are generated by the input process:

id	**field**	**value**
Version	uid	0
	value	The version
Job	uid	0
	value	The name of the job. This is the same as the name of the directory the job resides in on \\ROBERT\OUTPUT.
	addinfo	An email address

By giving the commands add <xxx> the following lines can be added.

id	**field**	**value**
Host	uid	A unique integer given to the line when it was created and larger than all other uids at that time.
	ipaddr	The ip address of the host.

Target	uid	A unique integer given to the line when it was created and larger than all other uids at that time.
	ipaddr	The ip address of the target.
Net	uid	A unique integer given to the line when it was created and larger than all other uids at that time.
	addinfo	The network in the format x.x.x.x/bb.
Domain	uid	A unique integer given to the line when it was created and larger than all other uids at that time.
	addinfo	The name of the domain.

When Robert is given a *do Task* command the input process generates an Order line that summarises the order and a number of *Task* lines that lists the individual tasks that should be scheduled to complete the order. The *Order* line has the following format:

id	**field**	**value**
Order	uid	A unique integer given to the line when it was created and larger than all other uids at that time.
	name	The name of the task ordered. If more than one task was ordered only the first is given followed by + (a plus sign).
	ipaddr	An optional IP address to perform the order on. If no IP address is given it means perform it on the IP addresses given in all the *Host* lines in the job.
	ports	An optional port or port range to perform the order on. If no port is given it means 0-65535
	addinfo	An optional email address to be notified when the order is complete.

and each of the *Task* lines has the form

id	**field**	**value**
Task	uid	The same as the uid field of the corresponding Order line name The name of the task to be executed.
	ipaddr	An optional IP address to perform the order on. If no IP address is given it means perform it on the ip addresses given in all the *Host* lines in the job.

	ports	An optional port or port range to perform the order on. If no port is given it means 0-65535
	value	The uid of the other lines relating to this task. These lines can contain scheduling information as well as test results.
	value2	The static priority of the task.

The scheduling can be controlled through JobControl lines that come in three different flavours

id	**field**	**value**
JobControl	uid	Generated when the line is written
	name	*maxrun*
	value	The maximum number of running tasks that should be allowed in the job at any moment.
JobControl	uid	Generated when the line is written
	name	*time*
	value	A time to stop scheduling tasks in the job (seconds since 1970).
	value2	A time to start scheduling tasks in the job (in seconds since 1970).
	addinfo	A time to add to the other two times when they have both expired (in seconds).
JobControl	uid	Generated when the line is written
	name	*stopmode*
	value	*strict* if running tasks should be killed when the job stops scheduling.

During scheduling the *distribute* process writes a number of lines to the file.

id	**field**	**value**
TaskScheduled	uid	The value from the corresponding *Task* line.
	value	The internal IP address of the test computer the task has been started on.
	value2	The process id that the task is running under on the

		test computer.
TaskTimeout	uid	The value from the corresponding *Task* line.
TaskCancelled	uid	The value from the corresponding *Task* line.
TaskQueued	uid	The value from the corresponding *Task* line.

When the task is run on a test computer the *taskman* process that runs the task adds a line just before the task starts and a line just after it ends

id	**field**	**value**
TaskStart	uid	The value from the corresponding *Task* line.
	ipaddr	The ipaddr from the corresponding *Task* line.
	ports	The ports from the corresponding *Task* line.
TaskEnd	uid	The value from the corresponding *Task* line.

The commercially available applications for performing the tasks in which the access security of the ports is tested are integrated in the present system by programs called *wrappers* because they so to speak are wrapped around the applications. The wrapper that performs the task writes a line just before it starts a test of a single host and after it has finished. If individual hosts are not relevant for the task the *ipaddr* field is left blank.

id	**field**	**value**
HostStart	uid	The value from the corresponding *Task* line.
	name	The name of the tool used to perform the task.
	ipaddr	The host that will now be tested.
	value	The version of the tool used to perform the task.
HostEnd	uid	The value from the corresponding *Task* line.

The wrappers also writes lines with the results of the task, informational lines as well as vulnerability lines. The vulnerability lines have the format

id	**field**	**value**
Vuln	uid	The value from the corresponding *Task* line.
	ipaddr	The host where the vulnerability was found
	ports	An optional port where the vulnerability was found
	value	The testcase id for the vulnerability.
	value2	The (or part of the) tool vulnerability id.
	addinfo	Data from the tool about the vulnerability.

Port scanners report their output with

id	field	value
TcpInfo	uid	The value from the corresponding *Task* line.
	ipaddr	The host.
	ports	The port(s).
	value	*open, closed* or *unknown.*
	addinfo	The reason for the conclusion in *value* if that is available.
UdpInfo	uid	The value from the corresponding *Task* line.
	ipaddr	The host.
	ports	The port(s).
	value	*closed* or *unknown.*
	addinfo	The reason for the conclusion in *value* if that is available.

The protocol identifier produces the following lines that are included in the jobinfo.csv file

id	field	value
Protocol	uid	The value from the corresponding *Task* line.
	ipaddr	The host.
	ports	A port.
	value	The detected protocol for the port.

The procedure for tracing the route of a host, Traceroute, writes:

id	field	value
TraceRoute	uid	The value from the corresponding *Task* line.
	ipaddr	The host.
	value	*icmp, udp* or *icmp and udp.*
	addinfo	The found route.

A host that responds to ping is in the jobinfo.csv file reported with

id	field	value
Ping	uid	The value from the corresponding *Task* line.
	ipaddr	The host.

addinfo	Output from ICMP tool	

An Rpc services found on ports results in the following lines:

id	field	value
RpcInfo	uid	The value from the corresponding *Task* line.
	ipaddr	The host.
	ports	Rpc service number
	value	*open*
	addinfo	The service name

Information about operating system (OS) type:

id	field	value
OsInfo	uid	The value from the corresponding *Task* line.
	ipaddr	The host.
	value	Possible operating system(s).

And lastly the lines relating to Netbios information:

id	field	value
NetbiosName	uid	The value from the corresponding *Task* line.
	ipaddr	The host.
	value	The Netbios name
NetbiosDomain	uid	The value from the corresponding *Task* line.
	ipaddr	The host.
	value	The Netbios domain

CLAIMS

1. A method for operating a computer system for examining the access security of communication ports of an external computer, the method comprising the steps of

(1) retrieving, by means of a first computer of the computer system, a unique data communication address of the external computer, at least one unique communication port identification as well as the data communication protocol of each of the at least one communication port from data storage means associated with the first computer,

(2) establishing a data communication connection between the first computer and a second computer of the computer system via a data communication network,

(3) communicating the data communication address of the external computer, the communication port identification(s) as well as the data communication protocol(s) of the communication port(s) from the first computer via the data communication connection to said second computer, whereupon the data communication connection between the first computer and said second computer is closed,

(4) establishing a data communication connection from said second computer via a data communication network to the communication port of the external computer in accordance with the previously communicated data communication address of the external computer,

(5) examining the access security of the communication port(s) of the external computer by means of a software application being designed thereto and being executed by said second computer, whereupon the data communication connection between said second computer and the external computer is closed,

(6) generating a set of test result data representing the outcome of said examination and storing the set of test result data within data storage means associated with said second computer,

(7) establishing a data communication connection between the first computer and said second computer of the computer system via a data communication network,

(8) communicating the set of test result data from said second computer via the data communication connection to the first computer, whereupon the data communication connection between the first computer and said second computer is closed, and

(9) storing said test result data within data storage means associated with the first computer.

2. A method according to claim 1, wherein the computer system comprises at least two second computers being operated by means of different common standard computer operating systems.

3. A method according to claim 1 or 2, wherein the computer system comprises at least two second computers which may operate concurrently according to the present method.

4. A method according to claim 3, wherein the at least two second computers operate concurrently employing an identical data communication address of the external computer, identical communication port identification(s) as well as identical data communication protocol(s) of the communication port(s).

5. A method according to any of claims 1-4, comprising a port identification procedure being performed by a second computer of the computer system prior to the step (1) of retrieving data from said data storage means associated with the first computer of the computer system, the port identification procedure identifying data communication protocol(s) of communication port(s) of the external computer and produce an output accordingly.

6. A method according to claim 5, comprising a port examining procedure being performed by a second computer of the computer system prior to the port identification procedure, the port examining procedure being adapted to detect whether data communication via each of the plurality of communication ports of the external computer is enabled and produce an output accordingly, said output being significant for which ports of the external computer the data communication protocols are identified by means of the port identification procedure.

7. A method according to any of claims 1-6, comprising a data location procedure being performed by a second computer of the computer system prior to the step (1) of retrieving data from said data storage means associated with the first computer of the computer system, the data location procedure identifying the location of specific types of data files on data storage means associated with the external computer and produce an output of test result data accordingly to the first computer of the computer system to be used for subsequent examinations of access security of the external computer to which the test result data pertains.

8. A method according to claim 7, wherein the data location procedure comprises the steps of

retrieving, by means of a first computer of the computer system, a unique data communication address of the external computer from data storage means associated with the first computer,

establishing a data communication connection between the first computer and the second computer of the computer system via a data communication network,

communicating the data communication address of the external computer from the first computer via the data communication connection to said second computer, whereupon the data communication connection between the first computer and said second computer is closed,

establishing a data communication connection from said second computer via a data communication network to the external computer in accordance with the previously communicated data communication address of the external computer,

examining data storage means associated with the external computer so as to identify the location of specific types of data files on data storage means associated with the external computer by means of a software application being designed thereto and being executed by said second computer, whereupon the data communication connection between said second computer and the external computer is closed,

generating a set of test result data representing the outcome of said examination and storing the set of test result data within data storage means associated with said second computer,

establishing a data communication connection between the first computer and said second computer of the computer system via a data communication network,

communicating the set of test result data from said second computer via the data communication connection to the first computer, whereupon the data communication connection between the first computer and said second computer is closed, and

storing said test result data within data storage means associated with the first computer to be used for subsequent examinations of access security of the external computer to which the test result data pertains.

9. A method according to any of the preceding claims, wherein the data communication protocol of the communication port of the external computer involves encryption, an encryption key is communicated in step (3) from the first computer to the second

computer, and said encryption key is used at least for encrypting communication from the second computer to the external computer during the examination in step (5).

10. A method according to any of the preceding claims, comprising initial steps of

retrieving from data storage means associated with a third computer of the computer system at least one unique data communication address of an external computer,

establishing a data communication connection between the third computer and said first computer via a data communication network,

communicating said at least one data communication address of the external computer(s) from the third computer via the data communication connection to the first computer, whereupon the data communication connection is closed, and

storing said at least one data communication address within data storage means associated with the first computer,

after which initial steps the remaining of the method is performed for said communicated at least one data communication address, the method further comprising the final steps of

establishing a data communication connection between the third computer of the computer system and said first computer via a data communication network,

retrieving test result data relating to at least one of said communicated at least one data communication address from data storage means associated with the first computer,

communicating said retrieved test result data from the first computer via the data communication connection to the third computer, whereupon the data communication connection is closed,

storing said test result data within data storage means associated with the third computer,

establishing a data communication connection between an external computer and the third computer via a data communication network,

retrieving said test result data from data storage means associated with the third computer,

encrypting said retrieved test result data by means of a first encryption key, and

communicating said encrypted test result data from the third computer via the data communication connection to the external computer, whereupon the data communication connection is closed.

11. A method according claim 10, wherein the set of test result data is deleted from the data storage means associated with said first computer immediately upon the set of data has been communicated to the third computer.

12. A method according claim 10 or 11, wherein the set of test result data is deleted from the data storage means associated with said third computer immediately upon the set of data has been communicated to the external computer.

13. A method according to any of claims 10-12, wherein unique identification of at least one communication port of the external computer is retrieved from data storage means associated with the third computer during the initial retrieving step, said unique identification of at least one communication port being communicated to the first computer during the initial communication step.

14. A method according to any of claims 10-13, wherein the data communication protocol(s) of at least one communication port of the external computer is retrieved from data storage means associated with the third computer during the initial retrieving step, said data communication protocol(s) being communicated to the first computer during the initial communication step.

15. A method according to any of claims 10-14, wherein test specification data relating to the type of examination to be performed of the access security of the communication port(s) of the external computer is retrieved from data storage means associated with the third computer during the initial retrieving step, said test specification data being communicated to the first computer during the initial communication step.

16. A method according to any of claims 10-15, wherein the initial steps further comprise the step of

retrieving from data storage means associated with the third computer of the computer system a predetermined start time and a predetermined end time,

the method further comprising the step of

controlling the examination of the access security of step (5) so that the examination is performed between said predetermined start time and said predetermined end time.

17. A method according to any of claims 1-9, further comprising the steps of

establishing a data communication connection between an external computer and the first computer via a data communication network,

retrieving said test result data from data storage means associated with the first computer,

encrypting said retrieved test result data by means of a first encryption key, and

communicating said encrypted test result data from the first computer via the data communication connection to the external computer, whereupon the data communication connection is closed.

18. A method according claim 17, wherein the set of test result data is deleted from the data storage means associated with said first computer immediately upon the set of data has been communicated to the external computer.

19. A method according to any of claims 5-18, wherein the port identification procedure comprises the steps of

(a) retrieving from data storage means associated with the first computer a unique data communication address of an external computer,

(b) establishing a data communication connection between the first computer and a second computer of the computer system via a data communication network,

(c) communicating the data communication address of the external computer from the first computer via the data communication connection to said second computer, whereupon the data communication connection between the first computer and said second computer is closed,

(d) establishing a data communication connection from the second computer via a data communication network to a communication port of the external computer,

(e) receiving a possible first response via the data communication connection from the external computer,

(f) evaluating the first response, which may be empty, by use of a first set of information stored within data storage means associated with the second computer and relating to first responses from communication ports, said evaluation producing a first evaluation result of one of the following types:

i) the protocol cannot be identified by the present identification procedure,

ii) the identity of the protocol is identified, and

iii) further communication is required for protocol identification,

(g) performing, in case the first evaluation result is of type iii), a process comprising the following steps:

(h1) retrieving, in case the first evaluation result is of type iii), a second command from data storage means associated with the second computer,

(h2) communicating said second command from the second computer via the data communication connection to the communication port,

(h3) receiving a second response via the data communication connection from the external computer,

(h4) evaluating the received second response by use of a second set of information stored within data storage means associated with the second computer and relating to second responses from communication ports, said evaluation producing a second evaluation result,

(j) generating a set of port identification data representing the outcome of said identification procedure and storing the set of port identification data within data storage means associated with said second computer,

(k) establishing a data communication connection between the first computer and said second computer of the computer system via a data communication network, and

(l) communicating the set of port identification data from said second computer to the first computer, whereupon the data communication connection between the first computer and said second computer is closed.

20. A method according to claim 19, wherein the set of port identification data is deleted from the data storage means associated with said second computer immediately upon the set of data has been communicated to the first computer.

21. A method according to claim 19 or 20, wherein the second evaluation result is of one of said types of first evaluation results, and the method further comprises the step of performing, in case the second evaluation result is of type iii), a process comprising steps being similar to (h1) to (h4) involving a third command, a third response, a third set of information and a third evaluation result.

22 . A method according to claim 21 and comprising one or more further processes comprising steps being similar to (h1) to (h4).

23. A method according to any of claims 19-22, wherein at least some of the protocols are common standard data communication protocols.

24. A method according to any of claims 19-23, wherein a plurality of said identification processes are performed concurrently employing an identical unique data communication address of the external computer as well as an identical unique communication port identification, each of the plurality of identification processes employing command(s) and set(s) of information being specific for a given data communication protocol so as to test the communication port of the external computer for a plurality of different data communication protocols concurrently.

25. A method according to claim 24, wherein ongoing identification processes of the plurality of identification processes are terminated in reply to an evaluation result of type ii) of any of the plurality of identification processes.

26. A method according to any of claims 19-25, comprising the step of

(m) retrieving from data storage means associated with the second computer a new unique communication port identification,

after which the steps according to the method with the exception of steps (a)-(c) are repeated using the new unique communication port identification instead of the prior port identification.

27. A method according to any of claims 19-26, wherein unique identification of at least one communication port of the external computer is retrieved from data storage means associated with the first computer during step (a), said unique identification of at least one communication port being communicated to the second computer during step (c), said unique identification of at least one communication port being significant for which ports of the external computer the data communication protocols are identified by means of the port identification procedure.

28. A method according to claim 26, wherein step (m) and the thereof following port identification procedure are performed for a multitude of communication port of the external computer, the method further comprising, prior to the first performance of step (d), the steps of

(c1) establishing a data communication connection from the second computer via a data communication network to one or more predetermined communication port(s) of the external computer,

(c2) receiving a possible first response from each of the predetermined communication port (s) via the data communication connection from the external computer, and

(c3) storing the first response(s) from the predetermined communication port(s) within data storage means associated with said second computer,

the method further comprising the step of at least once during or after the performance of the multitude of identification procedures of communication ports,

retrieving the stored first response(s) from the data storage means associated with the second computer,

repeating steps (c1) and (c2), and

performing a comparison of the obtained first response(s) from the predetermined communication port(s) with the retrieved first response(s) so as to detect a disruption of the ability to establish data communication connections between the second computer and the external computer.

29. A method according to any of claims 6-28, wherein the port examining procedure comprises the steps of

retrieving, by means of the first computer, a unique data communication address of the external computer from data storage means associated with the first computer,

establishing a data communication connection between the first computer and a second computer of the computer system via a data communication network,

communicating the data communication address of the external computer from the first computer via the data communication connection to said second computer, whereupon the data communication connection between the first computer and said second computer is closed,

establishing a data communication connection from said second computer via a data communication network to the external computer in accordance with the previously communicated data communication address of the external computer,

examining a plurality of communication ports of the external computer to detect whether data communication via each of the plurality of communication ports is enabled, said examination being performed by means of a software application being designed thereto and being executed by said second computer, whereupon the data

communication connection between said second computer and the external computer is closed,

generating a set of port status data representing the outcome of said examination and storing the set of test result data within data storage means associated with said second computer,

establishing a data communication connection between the first computer and said second computer of the computer system via a data communication network, and

communicating the set of port status data from said second computer to the first computer, whereupon the data communication connection between the first computer and said second computer is closed,

the communicated set of port status data being significant for which ports of the external computer the data communication protocols are identified by means of the port identification procedure.

30. A method according to claim 29, wherein the plurality of communication ports are examined in a non-successive order designed to prevent a safety system of the external computer from recognising a systematic examination.

31. A method according to claim 30, wherein communication ports having a communication protocol assigned therewith according to a common or de facto communication standard are arranged at the beginning of the non-successive order.

32. A method according to claim 30 or 31, wherein communication ports not having communication protocol assigned therewith according to the common or de facto communication standard are arranged in the non-successive order with less than four, preferably less than three and most preferred less than two such communication ports between the communication port in question and a communication port having a communication protocol assigned therewith according to the common or de facto communication standard.

33. A method according to any of claims 30-32, wherein communication ports not having communication protocol assigned therewith according to the common or de facto communication standard are arranged at the end of the non-successive order.

34. A method according to any of claims 29-33, comprising, prior to the examination of the plurality of communication ports, the steps of

(c1) establishing a data communication connection from the second computer via a data communication network to one or more predetermined communication port(s) of the external computer,

(c2) receiving a possible first response from each of the predetermined communication port (s) via the data communication connection from the external computer, and

(c3) storing the first response(s) from the predetermined communication port(s) within data storage means associated with said second computer,

the method further comprising the step of at least once during or after the examination of the plurality of communication ports,

retrieving the stored first response(s) from the data storage means associated with the second computer,

repeating steps (c1) and (c2), and

performing a comparison of the obtained first response(s) from the predetermined communication port(s) with the retrieved first response(s) so as to detect a disruption of the ability to establish data communication connections between the second computer and the external computer.

35. A method according to claim 34, wherein

the procedure of detecting a possible disruption is performed after the examination of each communication port,

the port examining procedure is halted upon a detection of disruption of the ability to establish data communication connections between the second computer and the external computer,

where after the examination is resumed on another second computer of the computer system excluding the communication port being examined immediately prior to the disruption was detected.

36. A method according to claim 35, comprising the steps of

store information about the order of examination of communication ports immediately prior to disruptions within data storage means of the computer system for a plurality of examinations of communication ports of external computers,

performing an analysis of said information by means of the computer system so as to identify a set of individual communication ports and sequences of communication ports

being likely to cause a disruption and a data set in accordance herewith is stored within data storage means of the computer system, and

arranging the non-successive order for subsequent examination of communication ports so that said individual communication ports are arranged at the end of the non-successive order and said identified sequences of communication ports are avoided.

37. A method according to any of claims 29-36, wherein the set of port status data is deleted from the data storage means associated with said second computer immediately upon the set of data has been communicated to the first computer.

38. A method according to any of the preceding claims, wherein the set of test result data is deleted from the data storage means associated with said second computer immediately upon the set of data has been communicated to the first computer.

39. A method according to any of the preceding claims, wherein the data communication connection(s) between the second computer and a communication port of the external computer is established via a public data communication network.

40. A method according to claim 39, wherein the external computer is a part of an external computer system having a common data communication pathway through which all data communication to and from computers of the external computer system passes, the method further comprising the steps of

establishing a data communication connection between a computer of the computer system and a computer of the external computer system, and

at least once prior to or during the performance of an examination of the access security of the communication port(s) receiving data from said computer of the external computer system so as to verify that the common data communication pathway of the external computer system is functioning.

41. A method according to any of the preceding claims, wherein the generated set of test results is stored within data storage means associated with the computer system for subsequent evaluation of the employed software application for examining the access security if said software application has been employed less than a predetermined number of times by the computer system, whereupon a counter within the computer system and pertaining to said software application is advanced with one step.

42. A method for operating a computer system for regularly repeated examination of the access security of communication ports of a plurality of external computers, wherein the computer system comprises a database stored on data storage means of the computer system, the database comprising record files of characteristics of each of the plurality of external computer systems as well as schedule data relating to a desired scheduling of said regular repeated examination, the method comprising the step of examining the access security of communication ports of each of the external computers on a regular basis according to the schedule data by means of the method according to any of claims 1-41.

43. A method according to claim 42 and further comprising the steps of

receiving input data relating to a specific vulnerability of the access security of communication ports of computers as well as test specification data for the type of examination to be performed of the access security of the communication port(s) of the external computer to test for the specific vulnerability, and

examining the access security with respect to the specific vulnerability according to the present method for each of the plurality of external computers without interfering with the scheduled regularly repeated examination of the access security.

44. A method according to claim 42 or 43 and further comprising the steps of

receiving input data relating to a specific vulnerability of the access security of communication ports of computers having a given set of characteristics as well as test specification data for the type of examination to be performed of the access security of the communication port(s) of the external computer to test for the specific vulnerability,

searching the database so as to select a subset of the plurality of external computers based on a matching of the characteristics stored in the database and the set of characteristics given in the receiving input data, and

examining the access security with respect to the specific vulnerability according to the present method for each of the external computers of the selected subset without interfering with the scheduled regularly repeated examination of the access security.

45. A method according to claim 43 or 44, wherein the step of examining the access security with respect to the specific vulnerability is preceded by the steps of

producing a request from the computer system to an external entity via a public data communication network, the request relating to the performance of said examination of one or more of said plurality of external computers, and

receiving a positive reply from the external entity to the request.

46. A method according to any of claims 42-45, wherein at least a part of the set of test result data generated by the regularly repeated examination of the access security of each of the plurality of external computers is stored on data storage means of the computer system for being retrieved and used for subsequent examinations of access security of the external computer to which the test result data pertains.

47. A method according to any of the preceding claims, wherein the execution of the software application employed in step (5) comprises the steps of

(5.1) repeatedly performing a specified communication with one of the communication port of the external computer, and

(5.2) determine whether the communication port in question provides a response to the communication.

48. A method according to claim 47 further comprising the step of

(5.3) repeating step (5.1) after a predetermined time period in case it is determined in step (5.2) that the communication port in question does not respond.

49. A method according to claim 47 or 48, wherein the computer system is adapted for having a communication connection established to an external entity via a public data communication network and receiving and executing instructions for ending the execution of step (5.1) or for repeating step (5.1).

50. A method according to claim 47 or 48, wherein the computer system under the conditions that

it is determined in step (5.2) that the communication port in question does not respond, and

the communication port in question does not respond a predetermined time period thereafter,

is adapted for establishing a second data communication connection via a data communication network and producing a communication accordingly.

51. A computer system comprising at least two general purpose computers having one or more computer programs stored within data storage means associated therewith, the computer system being arranged for as well as being adapted for performing the method of any of claims 1-50.

52. A computer system according to claim 51 comprising at least two computers each being arranged for as well as being adapted for performing as a third computer according to the method, said at least two computers having a common data storage means associated with each of said at least two computers, each of said at least two computers being adapted for storage of test result data within said common data storage means as well as being adapted for retrieval of test result data from said common data storage means.

53. A computer system according to claim 51 or 52 comprising at least two computers each being arranged for as well as being adapted for performing as a first computer according to the method.

54. A method for operating a computer system for identifying data communication protocol(s) of communication port(s) of an external computer, comprising an identification procedure having the steps of

(a) retrieving from data storage means associated with the computer system a unique data communication address of the external computer as well as a unique communication port identification,

(b) establishing a data communication connection from the computer system via a data communication network to a communication port of the external computer in accordance with the information retrieved in step (a),

(c) receiving a first response via the data communication connection from the external computer,

(d) evaluating the received first response, which may be empty, by use of a first set of information stored within data storage means associated with the computer system and relating to first responses from communication ports, said evaluation producing a first evaluation result of one of the following types:

i) the protocol cannot be identified by the present identification procedure,

ii) the identity of the protocol is identified, and

iii) further communication is required for protocol identification,

(e) performing, in case the first evaluation result is of type iii), a process comprising the following steps:

(f1) retrieving, in case the first evaluation result is of type iii), a second command from data storage means associated with the computer system,

(f2) communicating said second command from the computer system via the data communication connection to the communication port,

(f3) receiving a second response via the data communication connection from the external computer, and

(f4) evaluating the received second response by use of a second set of information stored within data storage means associated with the computer system and relating to second responses from communication ports, said evaluation producing a second evaluation result.

55. A method according to claim 54, wherein the second evaluation result is of one of said types of first evaluation results, and the method further comprises the step of performing, in case the second evaluation result is of type iii), a process comprising steps being similar to (f1) to (f4) involving a third command, a third response, a third set of information and a third evaluation result.

56. A method according to claim 55 and comprising one or more further processes comprising steps being similar to (f1) to (f4).

57. A method according to any of claims 54-56, wherein at least some of the protocols are common standard data communication protocols.

58. A method according to any of claims 54-57, wherein a plurality of said identification processes are performed concurrently employing an identical unique data communication address of the external computer as well as an identical unique communication port identification, each of the plurality of identification processes employing command(s) and set(s) of information being specific for a given data communication protocol so as to test the communication port of the external computer for a plurality of different data communication protocols concurrently.

59. A method according to claim 58, wherein ongoing identification processes of the plurality of identification processes are terminated in reply to an evaluation result of type ii) of any of the plurality of identification processes.

60. A method according to any of claims 54-59, comprising the step of

(g) retrieving from data storage means associated with the computer system a new unique communication port identification,

after which the steps according to the method with the exception of step (a) are repeated using the new unique communication port identification instead of the port identification obtained from step (a).

61. A method according to any of the preceding claims, wherein the data communication connection(s) between the computer system and a communication port of the external computer is established via a public data communication network.

62. A computer system comprising at least one general purpose computer having one or more computer programs stored within data storage means associated therewith, the computer system being arranged for as well as being adapted for performing the method of any of claims 54-61.

63. A computer program product being adapted to enable a computer system comprising at least one general purpose computer having data storage means associated therewith and being arranged suitably to perform the method of any of claims 54-61.

64. A method for testing the vulnerability of a device for performing data communication via a data communication network by using a given common data communication standard, comprising the successive steps of

(a) establishing a data communication connection between a computer and the device via a data communication network,

(b) generating a data package in which the combination of attributes is invalid according to the given common data communication standard,

(c) communicating said data package from the computer to the device,

(d) detecting whether the device is able to issue a proper response to a valid data communication from the computer system, and

(e) repeating step (b) with a new invalid combination if the device was tested positive in step (d).

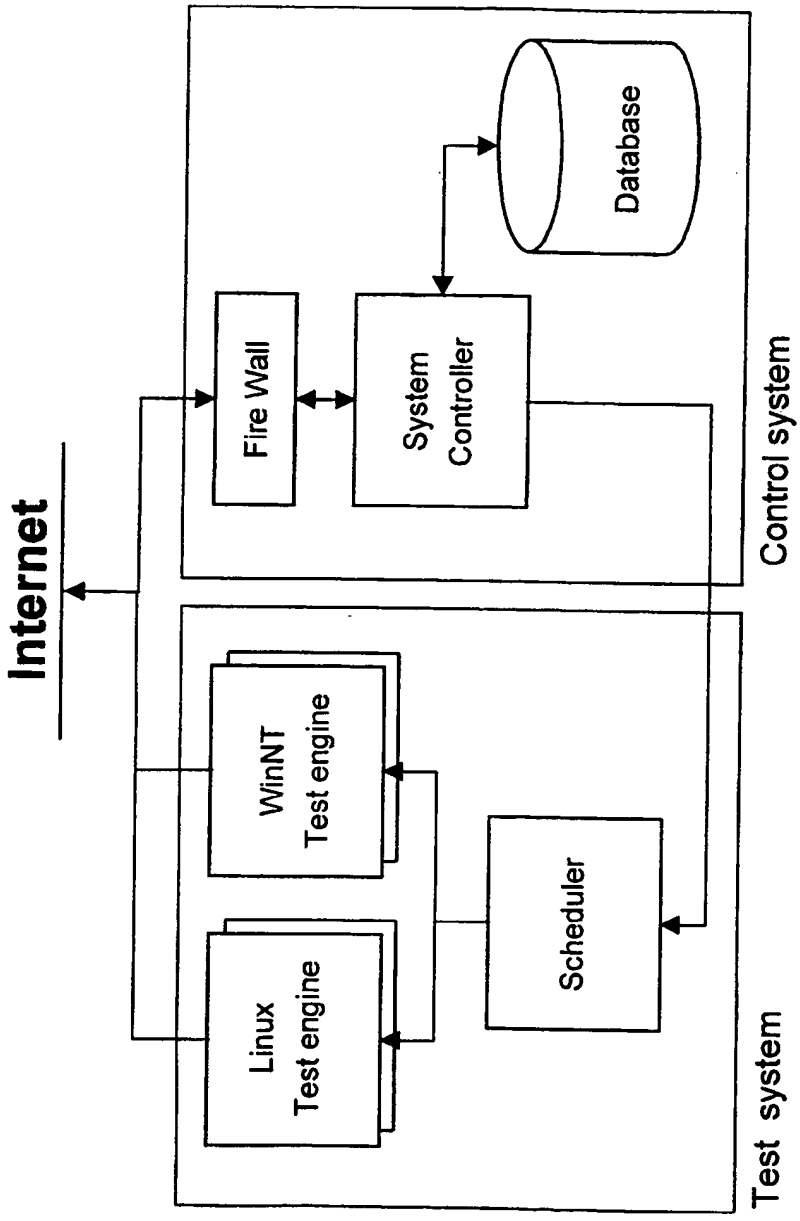
Internet
Fire Wall
System Controller
Database
Control system
WinNT Test engine
Linux Test engine
Scheduler
Test system

Fig. 1

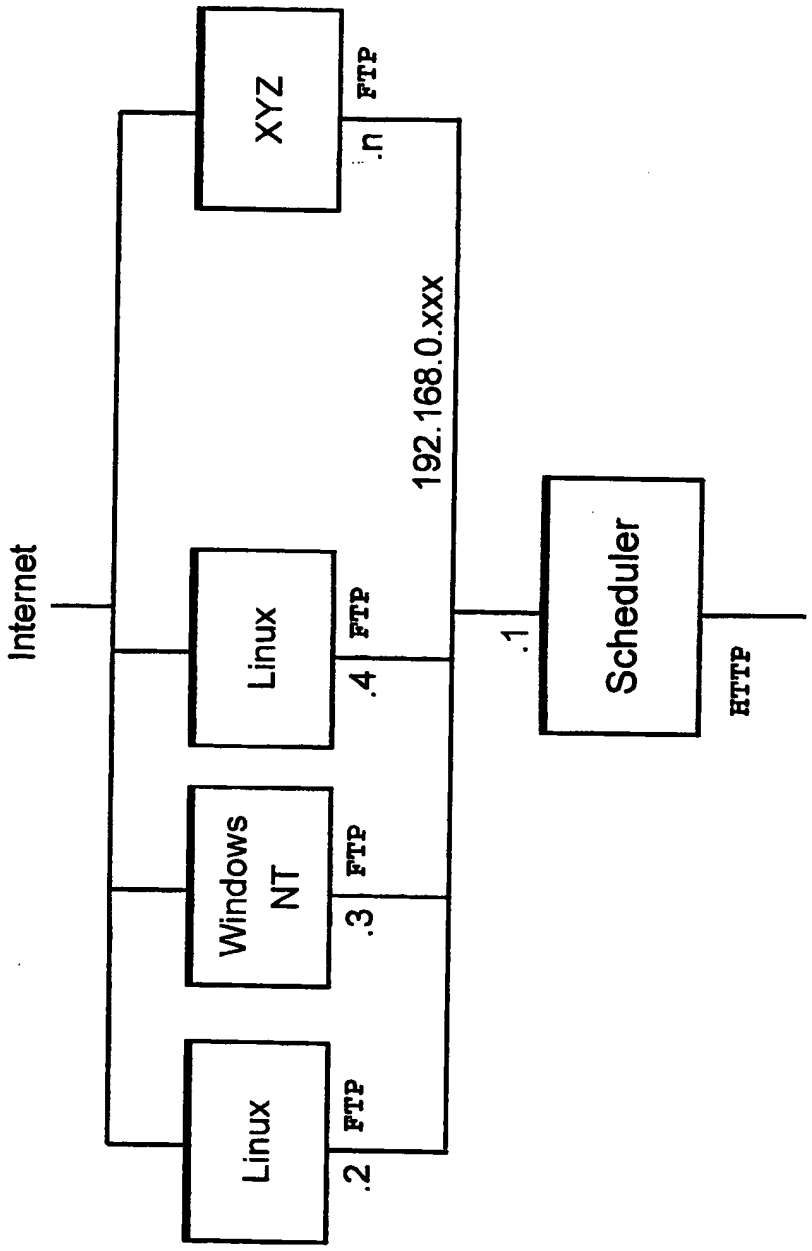
Internet
Linux
FTP
.4
Windows NT
FTP
.3
Linux
FTP
.2
XYZ
FTP
.n
192.168.0.xxx
.1
Scheduler
HTTP

Fig. 2

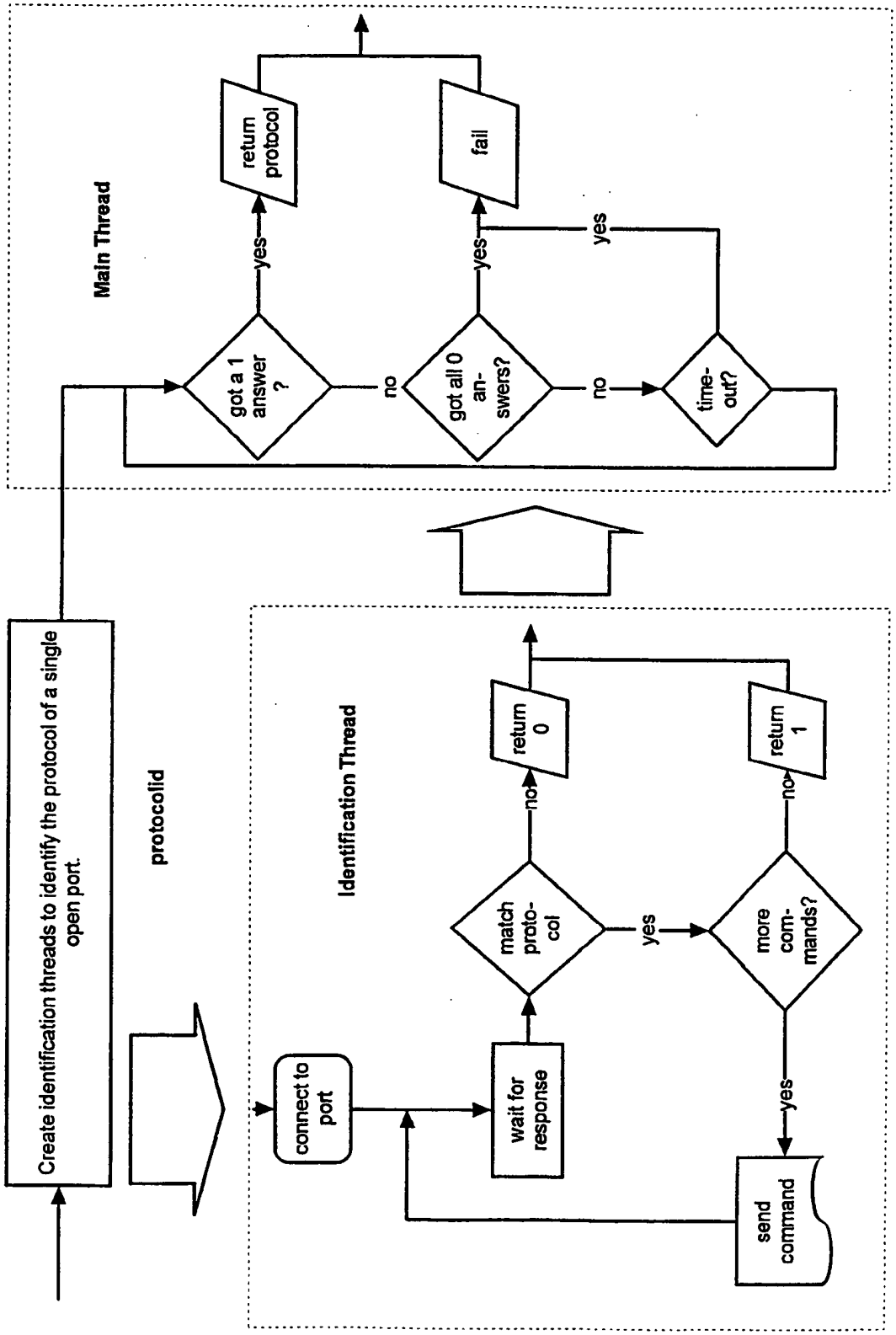
Main Thread
got a 1 answer ?
yes
return protocol
no
got all 0 answers?
yes
fail
no
time-out?
yes
Create identification threads to identify the protocol of a single open port.
protocolid
Identification Thread
connect to port
wait for response
match proto-col
no
return 0
yes
more com-mands?
no
return 1
yes
send command

Fig. 3